UNITED STATES PATENT APPLICATION

For

SYNCHRONIZING NETWORK SECURITY DEVICES WITHIN A NETWORK SECURITY SYSTEM

Inventor:

Hugh S. Njemanze

Prepared by:

Blakely, Sokoloff, Taylor & Zafman
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(408) 947-8200

Attorney's Docket No. 6388P011

"Express Mail" mailing label number: EV410137066US
Date of Deposit: December 10, 2003
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Vineta T. Tufono
(Typed or printed name of person mailing paper or fee)

Vineta T. Tufono
(Signature of person mailing paper or fee)

12-10-03
(Date signed)

SYNCHRONIZING NETWORK SECURITY DEVICES WITHIN A NETWORK SECURITY SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates to network security devices, and, in particular, a network security system analysing data from plurality of network security devices.

BACKGROUND

[0002] Computer networks and systems have become indispensable tools for modern business. Today terabits of information on virtually every subject imaginable are stored in and accessed across such networks by users throughout the world. Much of this information is, to some degree, confidential and its protection is required. Not surprisingly then, various network security monitor devices have been developed to help uncover attempts by unauthorized persons and/or devices to gain access to computer networks and the information stored therein.

[0003] Network security devices – also referred to as sensor devices, sensor products, security devices, and other similar names – largely include Intrusion Detection Systems (IDSs), which can be Network or Host based (NIDS and HIDS respectively). Other network security products include firewalls, router logs, and various other event reporting devices. Due to the size of their networks, many enterprises deploy many instances of these devices throughout their networks. Each network security device has a clock by which it tells time. However, these clocks may be out of synchronization with respect to each other.

SUMMARY OF THE INVENTION

[0004] Clocks used by network security devices can be synchronized by a network security system. In one embodiment, the synchronization can include the network security system receiving a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock. Similarly, the network security system can receive a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock. The system can then identify a common event represented by a first alert in the first stream from the first network security device and by a second alert in the second stream from the second network security device, and then synchronize the first clock and the second clock using the common event.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings in which like reference numerals refer to similar elements and in which:

[0006] **Figure 1** is a block diagram illustrating a network security system in which embodiments of the present invention may be implemented; and

[0007] **Figure 2** is a flow diagram illustrating clock synchronization according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0008] Described herein is a method and apparatus for synchronizing the internal clocks of various security devices of a network security system.

[0009] Although the present system will be discussed with reference to various illustrated examples, these examples should not be read to limit the broader spirit and scope of the present invention. For example, the examples presented herein describe distributed agents, managers and various network devices, which are but one embodiment of the present invention. The general concepts and reach of the present invention are much broader and may extend to any computer-based or network-based security system.

[0010] Some portions of the detailed description that follows are presented in terms of algorithms and symbolic representations of operations on data within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the computer science arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise, it will be appreciated that throughout the description of the

present invention, use of terms such as "processing", "computing", "calculating", "determining", "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0011] As indicated above, one embodiment of the present invention is instantiated in computer software, that is, computer readable instructions, which, when executed by one or more computer processors/systems, instruct the processors/systems to perform the designated actions. Such computer software may be resident in one or more computer readable media, such as hard drives, CD-ROMs, DVD-ROMs, read-only memory, read-write memory and so on. Such software may be distributed on one or more of these media, or may be made available for download across one or more computer networks (e.g., the Internet). Regardless of the format, the computer programming, rendering and processing techniques discussed herein are simply examples of the types of programming, rendering and processing techniques that may be used to implement aspects of the present invention. These examples should in no way limit the present invention, which is best understood with reference to the claims that follow this description.

Network Security System

[0012] With reference to Figure 1, an example of a computer-based network security system 100, in which an embodiment of the present invention can be implemented, is illustrated. Network security system 100 collects alerts from various network security devices 112. These device can include various IDSs 112A-C, which can be host or network based, firewalls 112D, routers 112E, and various other security devices and products 112F. These devices generate various alerts that represent physical events and incidents occurring in the network being monitored. Each of these devices has access to an internal or external clock that they can use to add timestamps to the generated alerts. In one embodiment, distributed agents of the network security system 100 collect these alerts.

[0013] Agents are software programs that provide efficient, real-time (or near real-time) local event data capture and filtering from a variety of network security devices and/or applications. The primary sources of security events are common network security products, such as the firewalls, intrusion detection systems and operating system logs described above. Agents can collect alerts from any source that produces event logs or messages and can operate at the native device, at consolidation points within the network, and/or through simple network management protocol (SNMP) traps.

[0014] The network security system 100 can include a manager 114. In one embodiment, managers 114 are server-based components that further consolidate, filter and cross-correlate alerts received from the agents, employing a rules engine 118 and a centralized event/alert database 120. One role of manager 114 is to capture and store all

of the real-time and historic event data to construct (via database manager 122) a complete, enterprise-wide picture of security activity. The manager 114 also provides centralized administration, notification (through one or more notifiers 124), and reporting, as well as a knowledge base 128 and case management workflow. The manager 114 may be deployed on any computer hardware platform and one embodiment utilizes a relational database management system such as an Oracle™ database to implement the event data store component. Communications between manager 114 and the distributed agents may be bi-directional (e.g., to allow manager 114 to transmit commands to the platforms hosting agents) and encrypted.

[0015] Consoles 116 are computer- (e.g., workstation-) based applications that allow security professionals to perform day-to-day administrative and operation tasks such as event monitoring, rules authoring, incident investigation and reporting. Access control lists allow multiple security professionals to use the same system and event database, with each having their own views, correlation rules, alerts, reports and knowledge base appropriate to their responsibilities. A single manager 114 can support multiple consoles 116.

[0016] In some embodiments, a browser-based version of the console 116 may be used to provide access to security events, knowledge base articles, reports, notifications and cases. That is, the manager 114 may include a web server component accessible via a web browser hosted on a personal or handheld computer (which takes the place of console 116) to provide some or all of the functionality of a console 116. Browser access is particularly useful for security professionals that are away from the consoles 116 and

for part-time users. Communication between consoles 116 and manager 112 is bi-directional and may be encrypted.

[0017] As mentioned above, the rules engine 118 is used to correlate alerts to produce meta-alerts, i.e., higher level alerts. For example, one rule may be that if twenty or more unsuccessful logins are followed by a successful login from the same IP address within a specified time window, then a high-level alert representing a successful brute force dictionary attack is generated. Such rules are generally expressed as Boolean expressions, but can be expressed using expressions with different formats as well.

[0018] Many rules incorporate a temporal element. As implied above, twenty unsuccessful logins from one IP address during a year does not raise suspicions. People mistype their passwords on a regular basis. However, twenty unsuccessful logins within one minute begins to look like an attack, an unauthorized person (or machine) guessing at a password. To enable the execution of such time-sensitive rules, each alert generally includes a timestamp indicating when the respective security device detected the event reported by the alert. Each security device uses its own local clock to generate these timestamps.

[0019] An example is now given of how the performance of the network security system 100 may be reduced when the local clocks of the security devices 112 reporting to the system 100 are not synchronized. In this example, one rule of the rules engine 118 states that, if ALERT B is seen within 5 seconds of ALERT Y, then a high-level ALERT V is produced. For the purposes of this example, during the thirty second timeframe between 08:09:00 and 08:09:30, the agent manager 126 collects the following alerts from IDS1, as shown in Table 1:

Table 1 – Alerts From IDS1

Alert Name	Time of Detection (according to IDS1)
A	08:09:03
B	08:09:10
C	08:09:17
D	08:09:22

[0020] During the same timeframe the agent manager 126 also collects the following alerts from IDS2, as shown in Table 2:

Table 2 – Alarms From IDS2

Alert Name	Time of Detection (according to IDS2)
X	08:09:07
Y	08:09:16
Z	08:09:20
W	08:09:26

[0021] Form the data in Tables 1 and 2 above, it appears that ALERT B has not been seen within five seconds of ALERT Y, since ALERT B was detected six seconds before ALERT Y. Thus, the rules engine 118 would not correlate the two alerts to produce high-level ALERT V. However, if the clock used by IDS2 is two seconds ahead of the clock used by IDS1, then, in reality, the event giving rise to ALERT Y occurred only four seconds after the event giving rise to ALERT B. Thus, had the clocks been in

synchronization, the rule should have been activated. Thus, the performance of the network security system was reduced because of this synchronization error.

Synchronizing Security Devices

[0022] One embodiment of the present invention is now described with reference to Figure 2. The simplified example of IDS1 and IDS2 from the preceding section is also used to demonstrate security device synchronization according to one embodiment of the invention. In block 202, the manager 114 is receiving alerts representing various security events observed by a first security device, e.g. IDS1. At the same time, in block 204 the manager 114 is receiving alerts representing various security events observed by a second security device, e.g. IDS2.

[0023] In block 206, the manager 114 identifies a common event. In one embodiment, a common event is an event that is represented by an alert from both of the two security devices. The manager 114 may use a software module, such as synchronization module 130 in Figure 1, to perform common event detection, and other synchronization related tasks. An example of a common event can be an XMAS scan event with the same source and target IP address detected separately by a Firewall and an IDS.

[0024] In one embodiment, a common event is detected when the same new source or target IP address is observed within a certain timeframe by two separate security devices. For example, if the first device observes a new target IP address at 10:10:05 and the second device observes the same new target IP address at 10:11:00, then a common event may be inferred. The timeframe should not be so narrow that all

common events are missed unless the clocks are already synchronized, nor so wide that separate events are inferred to be common events. In one embodiment, the user of the system 100 can configure this common event detection timeframe.

[0025] In another embodiment, common events can be detected by observing corroborative alerts from similar devices within the timeframe discussed above. For example, if two IDS devices from different manufacturers report similar alerts at around the same time, a common event can be inferred. These common alert detection methods, and other similar methods, are not mutually exclusive and can be used concurrently. In one embodiment, the user of the system 100 can configure the common event detection rules, and is allowed to author new rules.

[0026] After a common event is identified, it can be used, in block 208, to synchronize the clocks of the two devices. For example, with reference to the example in the section above, if a common event is identified with respect to ALERT A and ALERT X (in other words, if both alerts are found to be representations of the same event), then it can be inferred that they were detected at the same time. Since the time of detection of ALERT A is four seconds prior to the time of detection of ALERT X, it can be further inferred that the clock in IDS2 is four seconds ahead of the clock in IDS1. This information can then be used to synchronize the two clocks.

[0027] In one embodiment, synchronizing the two clocks can be accomplished by making the two clocks meet in the middle. For example, the clock of IDS1 would be advanced by two seconds and the clock of IDS2 would be decreased by two seconds.

[0028] In another embodiment, one of the two device clocks would be designated a reference clock, and the other clock would be adjusted to the reference clock. For

example, if the clock of IDS2 were selected to be the reference clock, then the clock of IDS1 would be advanced by four seconds. There can be various ways to select which clock should be the reference clock. In one embodiment, the decision can be arbitrary or random.

[0029] In another embodiment, deciding which of the clocks should be the reference clock for a particular adjustment depends on the relationship of the clocks to the main system-wide reference clock. A real world network security system 100 has more than two sensor devices 112 whose clocks can be synchronized using the present invention. For example, consider a system with five such security devices 112, labelled Device1 to Device5. In this system, the system-wide reference clock is the clock of Device3.

[0030] Therefore, if one of the two devices 112 whose alarms represent the common event that is used to synchronize the clocks of these two devices is Device3, the clock of the other device 112 will be the one to be adjusted. In other words, between Device3 and any other device 112, the clock of Device3 will be the reference clock. However, what if the clock of Device1 is being synchronized with the clock of Device2.

[0031] If neither of the clocks to be synchronized is the system-wide reference clock, then, in one embodiment, the clock that has been most recently synchronized with the system-wide reference clock will be selected as the reference clock. For example, if Device2 has been recently synchronized with Device3, but Device1 has not, then the clock of Device2 is selected as the reference clock to which the clock of Device1 is adjusted. Many other such rules are possible to select the reference clock between the clocks being synchronized.

[0032] The discussion of Figure 2 has assumed for simplicity that only two security devices 112 are being synchronized at a time. However, a common event can trigger alerts from many devices, allowing one of them to be designated as a reference clock to which the clocks of the other devices 112 can be adjusted. Thus, a common event reported by a subset of all network security devices 112 can be used to synchronize the entire subset of devices 112.

[0033] Furthermore, a common event that would trigger alerts from all, or substantially all, sensor devices 112 could be effectively used to synchronize all, or substantially all, the devices 112 at once. In one embodiment, one or more events are purposefully injected into the network being monitored by the security devices 112. Such a synchronization event can be designed to elicit alerts from a large number of the devices 112. In this manner, many of the devices 112 can be synchronized with one common, albeit induced, event.

[0034] For simplicity, the discussion of Figure 2 has also assumed that the clocks of the individual devices 112 will be adjusted forward or backward. In a real world system, however, the network security system 100 may not have access to the clocks of the security devices 112. For example, IDS 112A may be a proprietary box that connects to a network, monitors the network, and generates alerts based on network activity. Its internal clock is not accessible for reprogramming by the manager 114. Indeed, if the clocks of all of the devices were accessible to the manager 114, the manager could synchronize all these clocks with the manager clock without detecting common events.

[0035] Thus, in one embodiment, at least some of the clocks to be synchronized using embodiments of the present invention are not accessible to a real life network

security system 100. In one embodiment, the manager 114 can synchronize these clocks by keeping a clock database that stores the offsets for each clock relative to the system-wide reference clock. For example, assume that the clock of router 112E is determined to be five seconds behind the clock of IDS 112A, the clock of Firewall 112D is determined to be two seconds ahead of the clock of IDS 112A, and IDS 112A is the system-wide reference clock, the clock database will so indicate, e.g., by associating +5 with Router 112E, and –2 with Firewall 112D.

[0036] In one embodiment, the clock database can be maintained by, and be accessible to the synchronization module 130. Thus, the synchronization module 130 can perform synchronization by adjusting entries in the clock database. Furthermore, the synchronization module 130 can correct the timestamps of the alerts based on the clock database. In the example above, each timestamp from Router 112E would be replaced by a timestamp that has been incremented by five seconds to compensate for the five second lag of Router 112E with respect to IDS 112A.

[0037] Thus, a method and apparatus for synchronizing security devices being monitored by a network security system have been described. In the forgoing description, various specific modules, such as the "synchronization module," have been described. However, these names are merely to describe and illustrate various aspects of the present invention, and in no way limit the scope of the present invention. Furthermore, various modules, such as the manager 114 and the synchronization module 130 in Figure 1, can be implemented as software or hardware modules, or without dividing their functionalities into modules at all. The present invention is not limited to any modular architecture, whether described above or not.

[0038] In the foregoing description, the various examples and embodiments were meant to be illustrative of the present invention and not restrictive in terms of heir scope. Accordingly, the invention should be measured only in terms of the claims, which follow.